The Art of the Breach

A journey from sidewalk to executive filing cabinet highlighting three different approaches to achieve our objective.

Passive entry: Social engineering

Covert entry: Lockpicking

Forced entry: What ever it takes

The Art of the Breach

Founder: Nonprofit Crowdsourced OSINT for Missing Persons
www.tracelabs.org

Profession: Senior IT Manager, Aerospace Industry
www.linkedin.com/in/robertsell

Volunteer: Coquitlam Search & Rescue: *Tracker*
www.coquitlam-sar.bc.ca

Twitter: @robertesell
Email: robertesell@gmail.com

The Art of the Breach

Housekeeping:

- **Standard disclaimer:** None of this material or ideas in no way represent employers or even potential employers from past, present or future.

- **Risk of Incarceration:** Physically breaking into a building without authorization from the owner is strictly forbidden. It is physically dangerous, costly and depending on your local laws, almost certainly criminal.

This content is being provided so that you may have a better understanding of criminal breach methodologies, allowing your organization to better prepare to defend against it.

The Art of the Breach

1. Research Target
2. Prepare Pretexts
3. Onsite Reconnaissance
4. Front/Back Door
5. Lobby
6. Elevator/Stairs/Hallway
7. Executive Office
8. Escape and Evade

The Art of the Breach

1 Research Target

Passive reconnaissance / Zero touch recon:

- Start at a high level and drill down into details
- Prepare before you start:
  - VM for dedicated and archivable platform
  - Sock puppets or correct settings
  - VPN (not just for privacy but also for location)
  - Organize your intelligence

The Art of the Breach

1 Research Target

Understand their business:

- Type of business
- Projects, products and services
- Population:
  - # of employees, executives, social butterflies
- Departments
- Vendors: document shredding, garbage, plant care

The Art of the Breach

1 Research Target

Understand their Infrastructure:

- Internet provider, parking, property management
- Floor plans
- First responders key boxes
- Cafeteria or gym
- HVAC (on roof)
- Ingress/Egress points (loading dock)
- Magnetic locks/Power outage:
  - Doors failing secure or failing open?
- Perimeter layers:
  - Fences, walls, man traps, terrain traps, CCTC

The Art of the Breach

1 Research Target

Understand their Defences:

- Guards
- Alarms
- CCTV
- Access cards
- Types of door locks
- Patterns of life (movement, schedules, hours)
- Sources:
  - YouTube videos of office tours,
  - employee social media, news

The Art of the Breach

2 Prepare Pretexts

Build pretexts on what was discovered in Stage 1:

- New employee or contractor
- Parking company attendant doing maintenance/survey
- Internet technician planning new fiber run
- Garbage or document shredding
- HVAC technician
- New personal trainer, janitor or plant care technician
- Security guard

The Art of the Breach

2 Prepare Pretexts

Tips: Look like you belong. Look boring and predictably mundane (grey man).

Backup pretexts if you get caught:

- You caught me! Congratulations. I was hired to test your defenses!
- Property management representative doing a lock test
- Locksmith hired to fix broken lock
- Locked out of my office
- Just a random employee who thought they would try this out

The Art of the Breach

3 Onsite Reconnaissance

- At this point we know:
  - the company, the building and the people.
- Arrive onsite and case the building
- any recent changes?
- Trust (our research) but verify.
- We want to eliminate surprises
  - before we commit to the breach.
- Careful not to expose ourselves
  - CCTV and employees.

The Art of the Breach

3 Onsite Reconnaissance

Look for:

- What is new or changed
- Doors and lock upgrades
- Guards and CCTV
- New patterns of life:
  - new smoking area, new eating area, movement.
- New defenses: man traps, alarms,
- New opportunities:
  - construction, vendors, out of order areas

The Art of the Breach

4 Front Door(s)

Since our operation is lengthy and complex, a stealthy approach may be beneficial where ever possible to avoid detection.

- Front door = highest amount of surveillance
- Funnels foot traffic and may include a man trap
- May have active guards and/or reception
- May force interaction with organization representative
- If successfully passed, legitimizes pretext

The Art of the Breach

4 Front Door(s)

Passive Entry Method 1: Have Access Card

- Clone an employee NFC key card for easy entry.
  - Ideally, we do a pre-visit as a door security contractor to setup an RFID credential skimmer (ESP key) which is an interception tool placed behind the card reader panel. Installation is a 5 minute job. 99% of these don't have tamper alarms so low risk. Once installed, it collects creds and sends via wifi to your phone.
- Walk in with cloned card, like you own the place (cause now you do).

The Art of the Breach

4 Front Door(s)

Passive Entry Method 2: Don't have Access Card

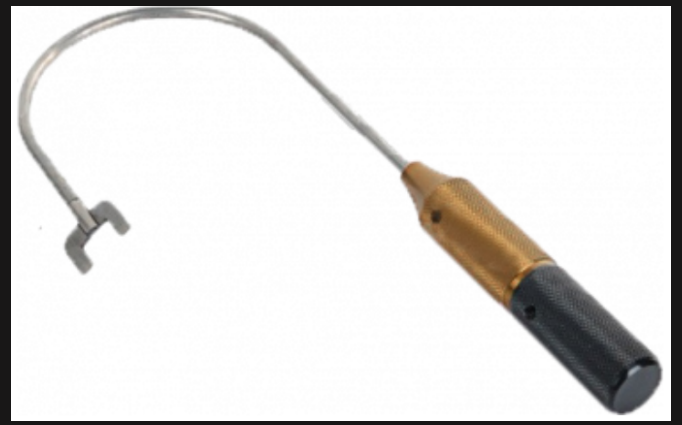
- Utilize most appropriate pretext for entry
- Match schedule or call in the day before
  - allows you to be expected
- Bag with multiple costumes provides flexibility
- Props allow excuse to ask others to open the door
- Tools can be used for Covert & Forced Entry techniques
- If successful, allows you to stay in Passive Entry mode

The Art of the Breach

4 Front Door(s)

Covert Entry Method

- Least preferred option on front door
- Will need some sort of cover to hide attack
- Much riskier than passive entry
- Need minimal time and disruption
- Building intelligence essential
- Options will depend on type of lock/door
  - Bypasses faster than picking
  - Thumb turn tool on glass doors



The Art of the Breach

4 Front Door(s)

Forced Entry Method

- Forced entry option best utilized at night
- Options depend on type of lock/door
- Forced entry to key access may be easier
- Alarm attack:
  - Likely already activated by forced entry
  - Use common codes such as 1234, 1212, 1379
  - Be prepared with employee pretext with alarm company if it triggers

The Art of the Breach

4 Front Door(s)

Forced Entry Method: Key boxes

- Often bylaw to provide a Fire Fighters Key Box. Exterior wall of the building in proximity to the principal entrance.
- Disadvantage: a single point of failure for security.
- February 2013 RSA Conference, a researcher publicized a possible exploit.
- Access to the key box gives an attacker keys to all doors. Success here gives you God Mode on the building.

A Knox-Vault in an academic building.

The Art of the Breach

Forced Entry Tools: The Metal Wedge

- Metal construction allows it to retain shape and pressure
- Great companion tool to increase effectiveness and speed of entry
- Helps create space (gap) allowing leverage - Prevents loss of gains

The Art of the Breach

Forced Entry Tools: Wedge Tip Wire Cutters

- Normally used by fireman to avoid entanglement risk
- Can also be used to shear small nails or screws
- Wedge like tip allows manipulation of screw ends in tight spaces

The Art of the Breach

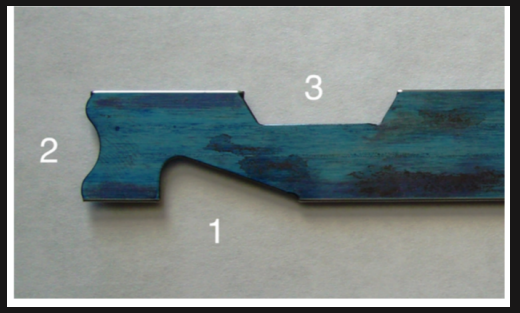
Forced Entry Tools: Modified Channel Lock Pliers

- Used to attack mortise cylinders. The only thing holding the mortise cylinder in place is a small set screw. Clam the jaw on, turn clockwise a quarter turn then counter clockwise until you completely spun out the cylinder. Once out, you can easily manipulate the locking mechanism with the modified handle.

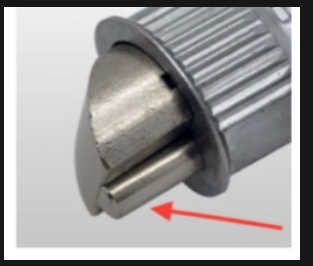

Mortise Cylinder

The Art of the Breach

Forced Entry Tools: The Shove Knife



- Used with both in and outward swinging doors
- Used on key in knob or spring latch type locks common to doors in offices
- Cut out 1: Outward swinging doors (toward you). If the latch is equipped with a tamper pin you may not be be able to defeat the latch with the shove knife.
- Cut out 2: Inward swinging doors. (away from you). Latch may be protected by a jamb (vertical support) which may need to be first removed.



The Art of the Breach

Forced Entry Tools: New York Roof Hook

- Tubular hollow shaft made from aircraft grade steel. Made for light/medium use. Not a pry bar or replacement for a halligan in forced entry.
- The chisel tip has a curve to provide leverage when prying.
- The opposite side of tool offers sloped sides that can be used like can opener.
- A deceivingly complex tool. Not for layperson but powerful in hands of expert.

The Art of the Breach

Forced Entry Tools: The Probar (Halligan)

- Drop forged 4120 steel means a light strong bar
- Excellent tool for forcing a door and performs well in confined space situations
- Must utilize the correct part of the tool for maximum mechanical advantage
- Up to 15 to 1 mechanical advantage can be generated.
- Hand position is important.

The Art of the Breach

4 Back Door(s)

Passive Entry Method: Loading Dock

- Opportunity for Passive Entry via social engineering
  - Smokers or delivery person
- Often void of man traps, guards and reception
- May require hard hat, steel toe shoes etc
- May offer an excellent egress option

The Art of the Breach

4 Back Door(s)

- Back door is often physically enforced and may require Covert or Forced Entry
- Could present opportunity for Passive Entry via social engineering
- Often void of man traps, guards and reception
- Does not necessarily legitimize pretext
- May offer an excellent egress option

The Art of the Breach

4 Back Door(s)

- Steel door with steel frame is common
- Simple key lock. No bolt heads indicating any other restriction.
- Forced entry: gap, set, force is the procedure to open.
- Use Probar (Halligan) as tool. Two person team ideal.
- Estimated time to breach: 2 minutes

The Art of the Breach

4 Back Door(s)

Covert/Forced Entry Method: Attacking the Hinges

- External doors are less favorable for hinge attack – Hidden defences
- Set screws may be stopping the removal of the pins
- Pins may have non removable pins like rivets and flattened on both ends
- Stud hinges or screw replacement studs can also defend the hinges
- Door may not open, even if you are successful at removing the pins
- If you think of a hinge as a lock, then its 3:1 – at best
- Broken hinges are is non reversable action

The Art of the Breach

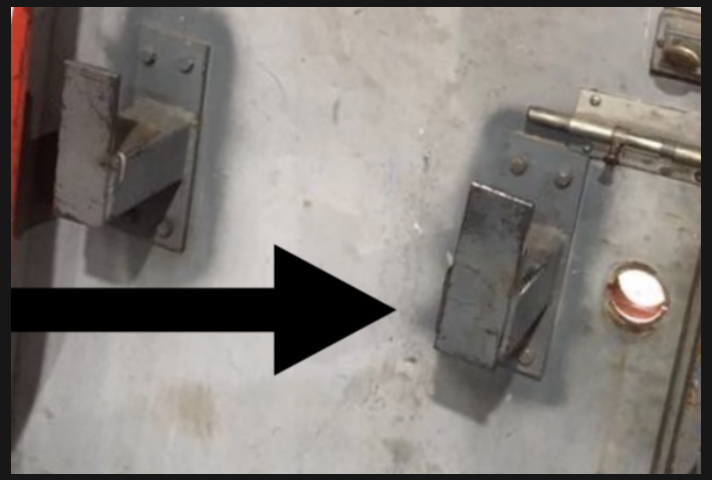
4 Back Door(s)

- Another steel door with steel frame
- Deadbolt PLUS pad lock
- Bolt heads indicate a drop arm behind the door
- Bolt heads are easily missed or dismissed
  - However represent a forced entry challenge

The Art of the Breach

4 Back Door(s)

- Use Probrar (Halligan) and circular saw
  - Cut lock and deadbolt
  - Discard then work drop arm
  - Options include: Simply drive the bolts through the door with irons, cut the bolts, grind the bolt heads off.
- Estimated time to breach: 6 minutes – 2 person team



The Art of the Breach

4 Back Door(s)

Forced Entry Method: Attacking Padlocks

Ramset Cobra + Nail Gun: Used to take .22 calibre now takes .27 calibre rounds

Model # 16942 Store SKU #1002226529

Best Seller

Ramset >

Cobra+ 0.27 Caliber Semi-Automatic Powder Actuated Tool with Silencer

★★★★☆ (74) Write a Review Questions & Answers (19)

- Power adjust drives pins flush
- Silencer reduces noise by 30% for better work environment
- Rubber cushion on grip means greater user comfort

$229.00

Save up to $100◇ on your qualifying purchase.
Apply for a Home Depot Consumer Card

No Country for Old Men

The Art of the Breach

5 Lobby

The lobby is a giant man trap as it likely has some of the following:

- Extensive CCTV (normally to cover all angles)
- Security guards
- Empowered employees
- Alarms
- Physical barriers
- Terrain traps such as human funnels

The Art of the Breach

5 Lobby

We want to either be:

1. Extremely comfortable entering and transitioning past; or

2. Not comfortable of the exposure and therefore avoid the lobby (alternate ingress point)

The Art of the Breach

6 Hallway

- Hallways are another form of man traps and can funnel the attacker.
- May offer cover from detection provided no one enter either side.
- No place to go if discovered so must be confident on movement.
  - Walk with purpose
  - Pretend your on the phone
  - Be looking at email to avoid eye contact

The Art of the Breach

6 Elevator

- Can be the perfect sanctuary if you have the key to control it
  - Out of service with controls
  - Sign on door
  - Sit in the elevator till after staff leaves
  - Emerge as the elevator repair technician
  - Egress option if you can control it

The Art of the Breach

6 Stairs

- Less people use the stairs so may offer some relief from detection
- May be a man trap
  - as floor entry likely requires entry card
- Floors may have access to specific individuals
- Cloned card for IT or Security may get you ever floor
- Pretext of Safety Inspector may be work for stairs

The Art of the Breach

7 Executive Office

- Close door and blinds to allow privacy
- Contained space provides level of safety
- Special ecosystem:
  - expect precision, tidiness and quality
- Pretext might need to change if caught
  - Why are we in the office or filing cabinet?

The Art of the Breach

7 Executive Office

Filing Cabinet - Passive entry:

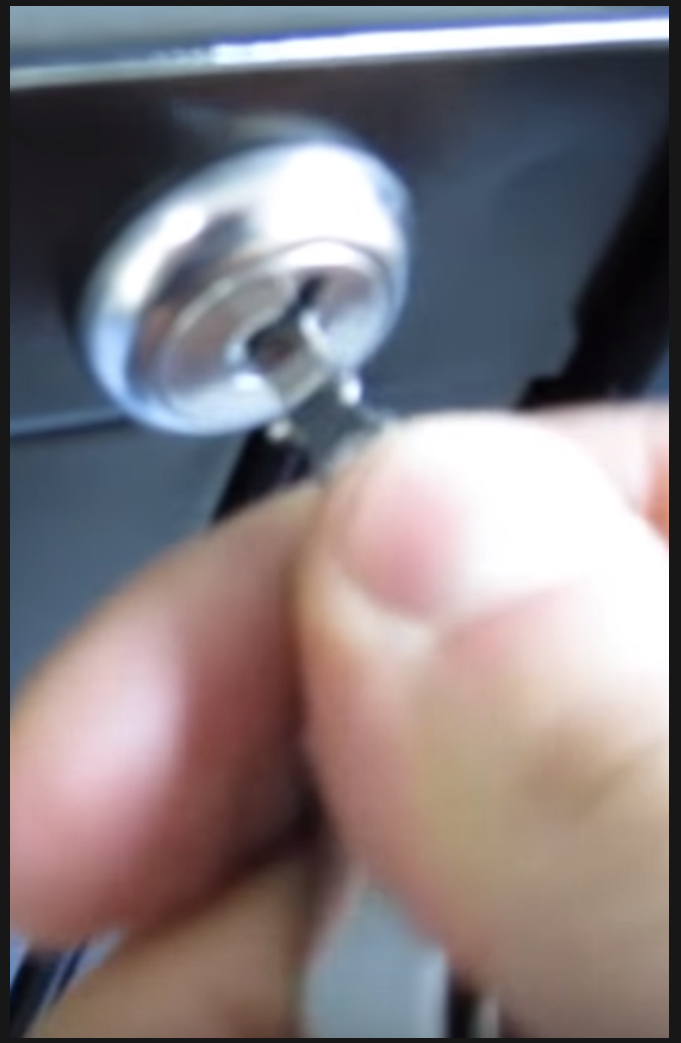
- Nail file or paper clip may be sufficient
- Tilt the cabinet over and push the rod
- Use the key (pre order or find)

Filing Cabinet - Covert entry:

- Use a bump key

Filing Cabinet - Forced entry:

- Drill the lock
- Impact the lock (hammer and screwdriver)



The Art of the Breach

8 Escape and Evade

- Leaving door ajar will allow us to simply push through
- Distractions may aid in not being detected:
  - fire alarm, first aid, etc
  - Don’t pretext fireman or law enforcement
- Moving with a crowd reduces risk
- Back of head to CCTV reduces future forensics risk
- Drop equipment, tools, clothing in common area
  - Retrieve later - Bathroom toilet tanks are ideal
- Unarmed security guards typically don’t detain

The Art of the Breach

References:

You're Probably Not Red Teaming… And Usually I'm Not, Either [SANS ICS 2018]: https://www.youtube.com/watch?v=mj2iSdBw4-0
How to open a door without keys: https://youtu.be/5mTYGfY0BhA
Forcible Entry for Glass Commercial Doors: https://youtu.be/MSQLDiboXCs
Commercial Rear Door Forcible Entry: https://youtu.be/7cEhNCjcxcg
Halligan bar demonstration: https://youtu.be/Pt7RPVoTd1E
Firefighter Forcible Entry: Pulling Hinges from a Metal Door and Jamb: https://youtu.be/uOPw94LYsgM
Inward Swinging Metal Door w/ Drop Bars - IRONS and LADDERS: https://youtu.be/1yCT_eDn34c
Door breaching: https://en.wikipedia.org/wiki/Door_breaching
Hardware Pentest Shop: https://sneaktechnology.com/
How to Bypass RFID Badge Readers: https://youtu.be/Ccm1caB6bao
8 Surprising Ways to Open Locks: https://youtu.be/7Lsm4l3mRqw
Cloning and Emulating RFID cards with Proxmark3: https://youtu.be/W22juSqhJSA
Dennis Maldonado - Real time RFID Cloning in the Field: https://youtu.be/kUduHIygbY8
Elevator Hacking: From the Pit to the Penthouse: https://youtu.be/ZUvGfuLlZus
File Cabinet Lock Picked and Bypassed: https://youtu.be/7R5VIz2U_MI
Life Hack 2 - How to easily pick a filing cabinet lock 2019: https://youtu.be/AhAJN8wSALo
Pick a Lock in SECONDS with a Bump Key: https://youtu.be/WpH_t0u5Ybg
RAMSET v MOUNTAIN Security DEADBOLT LOCK: https://youtu.be/1oPRYz5D9jo
STRONGER Ramset vs. Stronger Master Lock: https://youtu.be/YREflbQzVB4
The Pen-Sized Hinge Pin Destroyer: https://youtu.be/nJu_-Iuppc0
Lock pick tools: https://www.lockpicks.com/lock-entry-tools/lock-by-pass-tools.html

The Art of the Breach

Q & A